Documentation of System Weakness/Vulnerability and Associated Risk Level Based on NIST SP 800-30/Draft SP 800-30A

Principal Office: **System/Subsystem:** **Date:**
Weakness/Vulnerability:
Source that Identified Weakness/Vulnerability:

Mission Criticality of affected subsystem or system:
Critical ☐ **Important** ☐ **Supportive** ☐
Justification:

Data Sensitivity Impact Level of affected subsystem or system:
High ☐ **Moderate** ☐ **Low** ☐
Justification:

Overall Impact Rating (from Impact Table): **High** ☐ **Moderate** ☐ **Low** ☐

IMPACT TABLE (Page 23/Page 26)			
	Mission Criticality		
Data Sensitivity	**Supportive**	**Important**	**Critical**
High	*Low*	*Moderate*	*High*
Moderate	*Low*	*Moderate*	*Moderate*
Low	*Low*	*Low*	*Low*

THREAT LIKELIHOOD TABLE (Page 21/Page 24)			
	Countermeasure (affects opportunity)		
Threat Source (Affects motivation and means)	**High** Prevent or Significantly Impede	**Moderate** Impede	**Low** Ineffective
High Highly Motivated & Sufficiently Capable	*Low*	*Moderate*	*High*
Moderate Motivated & Capable	*Low*	*Moderate*	*Moderate*
Low Lacks Motivation or Capability	*Low*	*Low*	*Low*

Specific Counter Measure Applied:
Countermeasure Effectiveness: High ☐ **Moderate** ☐ **Low** ☐
Justification:

Threat Source: High ☐ **Moderate** ☐ **Low** ☐
Justification:

Overall Likelihood Rating (from Likelihood Table): **High** ☐ **Moderate** ☐ **Low** ☐

OVERALL WEAKNESS/VULNERABILITYRISK LEVEL (Page 25)

High ☐ Strong need for corrective actions as soon as possible
Moderate ☐ Need for corrective actions within a reasonable time period
Low ☐ Authorizing Official may correct or accept the risk

RISK LEVEL TABLE (Page 25/Page 29)			
	Impact		
Likelihood	**Low**	**Moderate**	**High**
High	*Low*	*Moderate*	*High*
Moderate	*Low*	*Moderate*	*Moderate*
Low	*Low*	*Low*	*Low*

_____ _____ _____ _____
Authorizing Official Date Certifying Official Date

Instructions for Documentation of System Weakness/Vulnerability and Associated Risk Level

BASIC INFORMATION

System/Subsystem should indicate whether the weakness/vulnerability that is documented on the form applies to the entire system or just a portion or subsystem. For example, a vulnerability/weakness that affects routers would impact the entire network. But vulnerability on print servers would only affect a less critical subsystem of the network. Please do not include full IP addresses or any other extremely sensitive data on the form. Provide just enough information to identify the system or subsystem affected.

Weakness/Vulnerability should include the type of weakness/vulnerability and a brief explanation of the potential damage it can cause. Please keep in mind that senior staff that may not have a deep technical background will review the form.

Source that identified Weakness/Vulnerability should indicate the tool that was used, if applicable (e.g., Nessus Vulnerability Scanner), and who discovered the weakness/vulnerability (e.g., system support staff, risk assessors, OIG). Please also include whether or not this is a repeat finding from an OIG audit. For instance, if system security staff complete scans that identify vulnerabilities that have been previously cited by the OIG, please indicate in which audit this vulnerability was cited.

IMPACT

Mission Criticality of affected subsystem or system cannot be higher than overall System Mission Criticality as determined by the Critical Infrastructure Protection (CIP) survey, but may be lower. For instance, a Mission Critical LAN may contain Mission Supportive subsystems such as some print servers or individual PCs.

Data Sensitivity Impact Level of affected subsystem or system cannot be higher that Confidentiality, Integrity or Availability rating (as appropriate) than that assigned to the overall system, or than the highest Impact rating if associated with more than one data sensitivity category. For instance,

LIKELIHOOD

Countermeasure is rated on effectiveness for removing opportunity through prevention or reducing the time of available opportunity due to detection. The definitions for High, Medium and Low are taken from the NIST Special Publication 800-30 (page 21 of NIST SP 800-30, and page 24 of the draft NIST SP 800-30A).

Threat Source is rated on motivation and skill capability (or means) of the threat source. The definitions for High, Medium and Low are taken from the NIST Special Publication 800-30 (page 21 of NIST SP 800-30, and page 24 of the draft NIST SP 800-30A). Please consider the following threat source categories:

Outside Threat Source has no authorized access
Basic Inside Threat Source has authorized access that matches the general access provided to the system
Privileged Inside Threat Source has authorized access beyond the basic user, such as a system administrator

OVERALL WEAKNESS/VULNERABILITY RISK LEVEL

The definitions for High, Medium and Low are taken from the NIST Special Publication 800-30 (page 25 of NIST SP 800-30, and page 29 of the draft NIST SP 800-30A). All high and moderate findings MUST be removed or reduced to a low risk.